Available online at www.sciencedirect.com
SCIENCE DIRECT®
ACADEMIC PRESS
Finite Fields and Their Applications 9 (2003) 150–156
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

On an open problem of Niederreiter

Qifan Zhang[1]

Department of Mathematics, Sichuan University, Chengdu 610064, China

Received 5 October 2000; revised 10 May 2002; accepted 17 July 2002
Communicated by Rudolf Lidl

Abstract

Niederreiter in 1991 proposed an open problem–to characterize the polynomials in $F_q[x_1, \ldots, x_n]$ which are permutation polynomials over every finite extension of F_q. The answer is well known for the case $n = 1$. In this paper the author studies it for the case $n = 2$ and solves the problem under a condition $\gcd(\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}) = 1$ and $\mathrm{Deg} f \not\equiv 0 \pmod p$

Keywords: Permutation polynomial; Finite field; Morphism; Embedding line theorem

1. Introduction

Throughout this paper k denotes a fixed algebraic closure of the field $\mathbb{Z}/p\mathbb{Z}$, and F_q denotes the subfield of k with q elements. A polynomial $f(x_1, \ldots, x_n)$ over F_q is called a *permutation polynomial* (PP for short) over F_q if the equation $f(x_1, \ldots, x_n) = a$ has exactly q^{n-1} solutions in F_q^n for all $a \in F_q$ (see [3]). By convention, a polynomial in $F_q[x_1, \ldots, x_n]$ which is a PP over every finite extension of F_q is called an *S-polynomial of* F_q. In 1963, Carlitz [2] discovered an S-polynomial in one variable should be of the form $ax^{p^h} + b$, where $a \neq 0$ and $h \geqslant 0$. Based on it, Niederreiter in 1991 proposed the open problem listed in the abstract of this paper, namely, to characterize all S-polynomials of F_q in n variables (see [4]).

There is a well-known Zeta function for a polynomial $f(x_1, \ldots, x_n)$ over F_q:

$$Z(f/F_q, T) = \exp \sum_{i=1}^{\infty} \frac{N_i}{i} T^i,$$

E-mail address: sszibbh@mail.sc.cninfo.net.
[1] This work is supported by NSFC, grant numbers (10128102, 19901023).

1071-5797/03/$ - see front matter
PII: S1071-5797(02)00008-4

where N_i denotes the number of the F_{q^i} rational points of the variety defined by f.

By the work of Weil, Dwork and Deligne, the zeta function is of good properties. Dwork attached a series of L-functions to a family of varieties over a finite field in order to understand how the roots of the zeta function vary when the variety moves through a family. Dwork's conjecture, proved by Wan, means the L-functions are p-adically meromorphic (see [5,6]). Clearly, f is an S-polynomial of F_q if and only if for every $a \in k$, the zeta function of the affine variety $f(x_1, \ldots, x_n) - a = 0$ over $F_{q^{\deg a}}$ is $\frac{1}{1-q^{(n-1)\deg a}T}$, where $\deg a$ denotes the least r such that $a \in F_{q^r}$. In this case we can compute explicitly the Dwork's L-functions of the family (of varieties) defined by f in a natural way:

$$L^{[r]}(f/F_q, T) = \prod_{\bar{a} \in \mathbf{A}^1(F_q)} \frac{1}{1 - q^{r(n-1)deg\, a} T^{deg\, a}} = \frac{1}{1 - q^{1+r(n-1)}T},$$

where $\bar{a}$ runs over the closed points of $\mathbf{A}^1(F_q) := \mathrm{spec} F_q[t]$, and a takes any geometric point corresponding to $\bar{a}$:

$$L^{[r]}(s, f, T) = 1, \quad \text{if } s \neq n-1$$

and

$$L^{[r]}(n-1, f, T) = \frac{1}{1 - q^{1+r(n-1)}T}.$$

This is one of the rare examples in which Dwork's L-functions can be computed explicitly. We can see these L-functions equal those of a trivial vector bundle. Niederreiter's problem can be expressed as follows:

What do the polynomials attached to the trivial L-functions look like?

The author in [7] gave a geometric characterization to S-polynomials in 2 variables. The author in this paper obtains the following further result:

Theorem. *Let* $f \in F_q[x, y]$, $\gcd\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = 1$ *and* $\mathrm{Deg} f \not\equiv 0 \pmod p$. *Then* f *is an S-polynomial if and only if there exists a* F_q*-automorphism* τ *of* $F_q[x, y]$ *such that*

$$f(x, y) = \tau\, x.$$

Remark. It is well known that every endomorphism τ of $k[x, y]$, in a standard way, corresponds to a unique endomorphism σ of $\mathbf{A}^2$. If σ is an endomorphism of $\mathbf{A}^2$ defined by

$$\sigma(x, y) = (u(x, y), v(x, y)),$$

the corresponding $\tau := \sigma^*$ is defined as

$$\tau f(x, y) = f(u(x, y), v(x, y)) = f(\sigma(x, y))$$

or

$$\tau(x,y) \coloneqq (\tau x, \tau y) = (u(x,y), v(x,y)).$$

To avoid confusion, σ always turns a point into a point, and τ always turns a polynomial into a polynomial. τ is an endomorphism of $F_q[x,y]$ if and only if σ is defined over F_q.

2. Preliminaries

At first, we recall some lemmas from [7].

Lemma 2.1. *Let $f \in F_q[x,y]$, then f is an S-polynomial of F_q if and only if $f = f_1^{p^h}$, where f_1 is an absolutely irreducible S-polynomial of F_q and $h \geqslant 0$.*

Lemma 2.2. *Let $f(x,y) \in F_q[x,y]$ be absolutely irreducible. Then f is an S-polynomial of F_q if and only if, for every $a \in k$, the curve $C : f(x,y) - a = 0$ is a rational curve with one place at infinity and the standard morphism $\phi : \tilde{C} \to C$ is one-to-one, where $\tilde{C}$ is the normalization of C.*

Lemma 2.3. *If $f(x,y)$ is an absolutely irreducible S-polynomial of F_q and* $\gcd\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = 1$, *then, for some $a \in k$, the affine curve $C : f(x,y) - a = 0$ is isomorphic to the affine line $\mathbf{A}^1$.*

Lemma 2.1 is an analogue of Carlitz's result, but there are too many absolutely irreducible polynomials in 2 variables. By Lemma 2.2, we see that f is an S-polynomial of F_q if and only if f is a PP over every finite field containing the coefficients of f. From now on, we can say a polynomial f in 2 variables over k is an S-polynomial (it means f is an S-polynomial of some finite subfield of k). Lemma 2.3 implies that it is necessary for us to study *imbedding lines* in $\mathbf{A}^2(k)$, namely the curves in $\mathbf{A}^2(k)$ isomorphic to the affine line. So we need the embedding line theorem and other relevant lemmas. The embedding line theorem, motivated by Jacobi's conjecture, is proved firstly by Abhyankar and Moh [1]. Some new proofs are given by Chang, Kang, Richman and others.

Lemma 2.4 (Embedding line theorem). *Let u and v be non-constant polynomials of degree n and m in t with coefficients in k. Assume that $k[t] = k[u,v]$, and* $\gcd(m,n) \not\equiv 0 \bmod p$, *then either m divides n or n divides m.*

Lemma 2.5. *Let u and v be polynomials satisfying the conditions of* Lemma 2.4, *and the curve $C : f(x,y) = 0$ can be parameterized as $x = u(t), y = v(t)$, then* $\deg_x f = m$, $\deg_y f = n$, $\mathrm{Deg} f = \max(m,n)$ *and $f(x,y)$ has the following form*:

$$f(x,y) = ax^m + \cdots + by^n,$$

where a, b are nonzero elements in k, $\mathrm{Deg} f$ denotes the degree of f as a two variables polynomial, and $\deg_x f$ denotes the degree of f as a polynomial in x with coefficients in $k[y]$.

Proof. Construct a homomorphism ϕ from $k[x,y]$ to $k[t]$ defined by

$$\phi(x) = u(t), \quad \phi(y) = v(t).$$

It follows that ϕ is surjective and its kernel is the ideal $(f(x,y))$, in other words, ϕ induces an isomorphism $\bar{\phi}$ from $k[x,y]/(f(x,y))$ to $k[t]$:

$$\bar{\phi}(\bar{x}) = u(t), \quad \bar{\phi}(\bar{y}) = v(t).$$

It is easy to see the minimal polynomial of t over $k(v(t))$ is $v(X) - v(t)$. It implies t satisfies the following properties:

$[k(t, v(t)) : k(v(t))] = m$, and t is integral over $k[v(t)]$.

So $u(t)$ satisfies the same properties. By the isomorphism $\bar{\phi}$, we can see that $\bar{x}$ is integral over $k[\bar{y}]$, and $[k(\bar{x}, \bar{y}) : k(\bar{y})] = m$. On the other hand, $f(x,y)$ is irreducible as a polynomial in 2 variables, so is $f(X, \bar{y})$ as a polynomial over $k(\bar{y})$. It implies $f(X, \bar{y}) = aX^m + a_1 x^{m-1} + \cdots + a_m$, where $a \in k^*$, $a_i \in k[\bar{y}]$. Hence $f(x,y) = ax^m + f_1(x,y)$, where f_1 is a polynomial satisfying $\deg_x f_1 < m$. Similarly, $f(x,y) = by^n + f_2(x,y)$ and $\deg_y f_2 < n$. So $f(x,y) = ax^m + g(x,y) + by^n$, where $\deg_x g < m$, $\deg_y g < n$. At last we show $\mathrm{Deg} f = \max(m,n)$. Without loss of generality, assume $m \geqslant n$. Write f as a sum $f = f_1 + \cdots + f_d$, where f_i is a homogeneous polynomial of degree i. Since the curve $C : f(x,y) = 0$ is isomorphic to the affine line, there should be only one point at infinity in the projective closure. So f_d is a power of a linear form. Thus $f_d = ax^d + \cdots$. Hence $m = d = \mathrm{Deg} f$.

3. The proof of theorem

Let G denote the group of k-automorphisms of $k[x,y]$, and E the set $k[t] \times k[t] - k \times k$. Given $\tau \in G$ and $(u,v) \in E$, we put $(u,v)^\tau = (f_1(u,v), f_2(u,v))$, where $(f_1(x,y), f_2(x,y)) = (\tau x, \tau y)$. This defines a right-action of G on E. For any u, v satisfying the condition of Lemma 2.4, we denote by ϕ_{uv} the corresponding homomorphism from $k[x,y]$ to $k[t]$. If $(u,v)^\tau = (u_1, v_1)$, then $(\phi_{uv} \circ \tau)(x,y) = \phi_{uv}(f_1(x,y),\ f_2(x,y)) = (f_1(\phi_{uv}(x), \phi_{uv}(y)),\ f_2(\phi_{uv}(x), \phi_{uv}(y))) = (u,v)^\tau = (u_1,\ v_1) = \phi_{u_1 v_1}(x,y)$

So

$$\phi_{u_1 v_1} = \phi_{uv} \circ \tau.$$

Now we can prove the theorem. The sufficiency is easy: an automorphism τ must correspond to an automorphism σ of $\mathbf{A}^2$ defined over F_q. $f = \tau x$ implies the map defined by f from $\mathbf{A}^2$ to $\mathbf{A}^1$ is the composite of σ and p_1, where p_1 is the projection

from $\mathbf{A}^2$ to $\mathbf{A}^1$. For every $a\in k$ and every finite field F_{q_1} containing $F_q(a)$, the set $f^{-1}(a)$ contains exactly q_1 F_{q_1}-points. Then we prove the necessity. By Lemma 2.3, we can find a suitable $a\in k$ such that the curve $C: f(x,y)-a=0$ is an imbedding line. Parameterize it as $x=u(t)$, $y=v(t)$, in other words, we have a surjective homomorphism ϕ_{uv} from $k[x,y]$ to $k[t]$ such that $\mathrm{Ker}\phi_{uv}=(f(x,y)-a)$. Without loss of generality assume $\mathrm{Deg} f=\deg_y f=n\geqslant m=\deg_x f>0$. By Lemma 2.5 we have $\deg u=n$ and $\deg v=m$. Since $n\not\equiv 0 \bmod p$, by Lemma 2.4 we have $m|n$ (of course $m\not\equiv 0 \bmod p$). Set $s=\frac{n}{m}$. Clearly, there exists $b\in k$ such that $\deg(u-bv^s)<n$. Keep doing so (noting $\deg v=m\not\equiv 0 \bmod p$), we get a polynomial ϕ_1 in one variable such that $\deg(u-\phi_1(v))<m$. Set $u_1=v$ and $v_1=u-\phi_1(v)$, i.e.,

$$(u_1,v_1)=(u,v)^{\tau},$$

where the k-automorphism τ is defined by $\tau(x,y)=(y,x-\phi_1(y))$. u_1 and v_1 still satisfies $k[u_1,v_1]=k[t]$, $\gcd(\deg u_1,\deg v_1)\not\equiv 0 \bmod p$, and $\deg u_1>\deg v_1$. Furthermore $\deg v_1>0$ as long as $\deg u_1>1$. Keep doing so, we get $(u_2,v_2),\ldots,(u_r,v_r)$ and $\tau_2,\ldots,\tau_r$ such that

$$(u_i,v_i)=(u_{i-1},v_{i-1})^{\tau_i}$$

and

$$(u_r,v_r)=(t,0).$$

So $\phi_{u_rv_r}=\phi_{uv}\circ\tau_1\cdots\tau_r=\phi_{uv}\circ\tau$, where $\tau:=\tau_1\cdots\tau_r$. Hence $\mathrm{Ker}\,\phi_{u_rv_r}=\tau^{-1}\mathrm{Ker}\,\phi_{uv}$. On the other hand, $\mathrm{Ker}\,\phi_{u_rv_r}=(y)$ and $\mathrm{Ker}\,\phi_{uv}=(f(x,y)-a)$. So

$$(f(x,y)-a)=\tau(y)$$

i.e.

$$f(x,y)-a=b\tau y,\quad b\in k^*,$$

$$f(x,y)=a+b\tau y=\tau(a+by)=\tau\tau_0 x,$$

where τ_0 is defined by $\tau(x,y)=(by+a,x)$. This implies the curve $f(x,y)=0$ is still an imbedding line, more precisely, the image of the line $x=0$ under the action of an automorphism of $\mathbf{A}^2$. But it is defined over F_q. So we can parametrize it by $u,v\in F_q[t]$. Repeat the preceding course we have $f(x,y)=\tau'(x)$, where τ' is a k-automorphism of $k[x,y]$, defined by polynomials over F_q. τ' induces in fact a F_q-automorphism of $F_q[x,y]$. This completes the proof of the theorem.

Remark. This proof gives an algorithm for f to determine τ such that $f=\tau x$. For a polynomial f satisfying the condition of the theorem, it is easy to check whether f is an S-polynomial. If f is an S-polynomial, we first change it, by a linear substitute, into a polynomial $f_1=y^n+g_1$, where $\mathrm{Deg}\, g_1<n$. Set $\deg_x f=m|n$, and $s=\frac{n}{m}$.

Choose a suitable $a \in F_q$ such that the degree of $f_2(x,y) = f_1(x + ay^s, y)$ is less than $\mathrm{Deg} f_1$. Keep doing so until we get the polynomial x. Thus, we find the τ such that $f = \tau x$. If we have to end before we get x, then f cannot be an S-polynomial.

4. Trivial examples and a kind of classification of polynomials in 2 variables

Clearly, there are many S-polynomials our theorem fails to characterize, say $x^p = \alpha^* x$, where α denotes the endomorphism of $\mathbf{A}^2$ defined by

$$\alpha(x,y) = (x^p, y).$$

We call σ a Frobenius map if σ is the composite of some endomorphisms, each of which is either an isomorphism or α. Thus, we get all trivial S-polynomials $\sigma^* x$ when σ runs through all Frobenius maps. If we identify f and $\sigma^* f$ for any Frobenius map σ and $f \in k[x,y]$, we get an equivalence relation $\sim$ in $k[x,y]$, which is the minimum equivalence relation satisfying the following properties:

(1) $f(x,y) \sim f(y,x)$,
(2) $f(x,y) \sim f(ax, y + \phi(x))$ for any $a \in k$ and $\phi \in k[x]$,
(3) $f(x,y) \sim f(x^p, y)$.

For any 2 elements f and g in $k[x,y]$ with $f \sim g$, and a sufficiently large field F_q, we have

$$L(f/F_q, T) = L(g/F_q, T), \tag{1}$$

because every Frobenius map is a bijection. In particular, f is an S-polynomial if and only if g is. The author believes that all S-polynomials are equivalent to each other.

Remark. Let $f : Y \to X$ be a family of algebraic varieties over F_q parametrized by X. For a rational number s and a natural number r, Dwork's rth power slope s L-function attached to the family f is defined as

$$L^{[r]}(s,f,T) = \prod_{\bar{x} \in X_0} \frac{1}{Z_s(Y_x/F_{q^{r\deg(x)}}, T^{\deg(x)})},$$

where X_0 denotes the set of the closed points of X, Y_x the fiber at x, and $Z_s(Y_x, T)$ the slope s part of the zeta function $Z(Y_x, T)$. (1) means that for any s and r,

$$L^{[r]}(s,f,T) = L^{[r]}(s,g,T).$$

Conjecture. *If $f \in k[x,y]$ is an S-polynomial, then $f \sim x$.*

Question. *For $f, g \in F_q[x,y]$, can condition* (1) *assure $f \sim g$?*

This question means whether the L-functions determine an equivalence class.

References

[1] S.S. Abhyankar, T.T. Moh, Embeddings of the line in the plane, J. Reine Angew. Math. 276 (1975) 148–166.
[2] L. Carlitz, Permutations in finite fields, Acta Sci. Math. Szeged 24 (1963) 196–203.
[3] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison–Wesley, Reading, MA, 1983.
[4] H. Niederreiter, Permutation polynomials in several indeterminates, in: G.L. Mullen, P.J. Shiue (Eds.), Finite Fields, Coding Theory and Advances in Communications and Computing, Marcel Dekker, New York, 1993, p. 433.
[5] D. Wan, A quick introduction to Dwork's conjecture, Contemp. math. 245 (1999) 147–163.
[6] D. Wan, Dwork's conjecture on unit root zeta function, Ann. Math. 15 (1999) 867–927.
[7] Qifan Zhang, Algebraic geometry's approach to permutation polynomials in several indeterminates, Algebra Colloq. 4 (4) (1997) 361–366.